BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-311674
(43)Date of publication of application : 28.11.1995

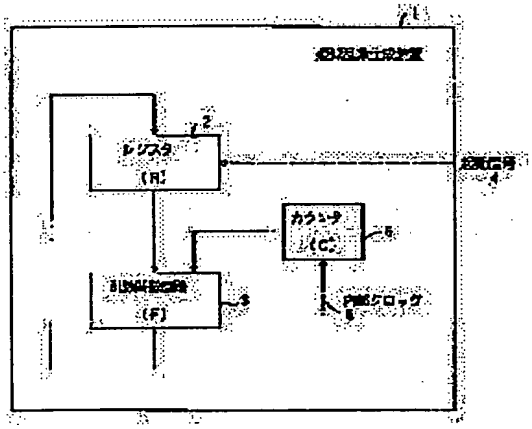
(51)Int.Cl. G06F 7/58
G09C 1/00
H04K 1/00
H04L 9/00
H04L 9/10
H04L 9/12

(21)Application number : 06-102988
(22)Date of filing : 17.05.1994

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : MORITA HIKARI
ABE MASAYUKI
AOYAMA MASAO

(54) PSEUDO-RANDOM NUMBER GENERATION DEVICE

(57)Abstract:
PURPOSE: To provide the pseudo-random number generation device which generates random numbers enabling safe key distribution, opposite-user confirmation, etc., while keeping the random numbers safe even under various conditions.
CONSTITUTION: The pseudo-random number generation device 1 is equipped with a counter 5 which counts a value C, a register 2 wherein a value R is stored, and a random number function circuit 3 which inputs the value C of the counter 5 and the value R of the register 2 and outputs a random number function F(R,C), and updates the value R in the register 2 with the random number function F (R,C) outputted from the random number function circuit 3 in response to a start signal.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－311674

(43)公開日　平成７年(1995)11月28日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	7/58	Ｂ			
Ｇ０９Ｃ	1/00		9364－5Ｌ		
Ｈ０４Ｋ	1/00	Ｚ			
Ｈ０４Ｌ	9/00				
				Ｈ０４Ｌ　9/00	Ｚ

審査請求　未請求　請求項の数３　ＯＬ　（全 ６ 頁）　最終頁に続く

(21)出願番号　特願平6－102988

(22)出願日　平成６年(1994)５月17日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号

(72)発明者　森田　光
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　阿部　正幸
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　青山　政夫
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

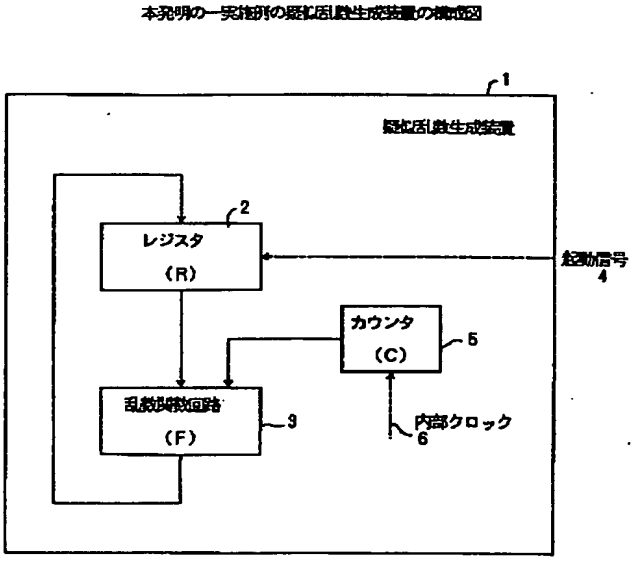
(74)代理人　弁理士　伊東　忠彦

(54)【発明の名称】　疑似乱数生成装置

(57)【要約】

【目的】　本発明の目的は、種々の条件下でも乱数の秘匿性を確保でき、鍵配送や、相手認証等が安全に実行できる乱数を生成する疑似乱数生成装置を提供することである。

【構成】　本発明の疑似乱数生成装置１は、値Ｃをカウントするカウンタ５と、値Ｒを蓄積するレジスタ２と、カウンタ５の値Ｃ及びレジスタ２の値Ｒが入力され、乱数関数Ｆ（Ｒ，Ｃ）を出力する乱数関数回路３とを具備し、起動信号を契機として乱数関数回路３から出力される乱数関数Ｆ（Ｒ，Ｃ）によりレジスタ２の値Ｒを更新する。



1

【特許請求の範囲】

【請求項１】　値Ｃをカウントするカウンタと、
値Ｒを蓄積するレジスタと、
該カウンタの値Ｃ及び該レジスタの値Ｒが入力され、乱数関数Ｆ（Ｒ，Ｃ）を出力する乱数関数回路とを具備し、
起動信号を契機として該乱数生成部から出力される該乱数関数Ｆ（Ｒ，Ｃ）により該レジスタの値Ｒを更新することを特徴とする疑似乱数生成装置。

【請求項２】　前記カウンタは、
内部クロックが前記起動信号と独立に与えられ、該内部クロックに基づいて逐次的に前記カウンタの値Ｃを更新する請求項１記載の疑似乱数生成装置。

【請求項３】　前記内部クロックは、外部からの観測不能とし、
前記カウンタは、前記内部クロックに基づいて逐次的にカウンタの値Ｃを更新することにより、外部から与えられる前記起動信号が前記カウンタの値Ｃを更新する周期と無関係に与えられる請求項１記載の疑似乱数生成装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、疑似乱数生成装置に係り、特に、暗号通信、鍵配送、相手認証等で必要となる乱数を生成する疑似乱数生成装置に関する。

【０００２】近年、２者間で通信において、相互に安全な鍵配送、相手認証等を行う端末や装置等のシステム中に内蔵される疑似乱数生成装置は、従来から求められている処理の再現性、計算機の資源のコンパクト化に加え、外部からの乱数値の類推が不可能な安全性の高さが求められている。

【０００３】

【従来の技術】鍵配送、相手認証等では、外部から推測できない安全な乱数が求められている。一般の乱数については、ＫＮＵＴＨ著：『準数値算法／乱数』（サイエンス社刊，ｐ３）で紹介されているように、処理の正当性の再現性、計算機資源のコンパクト化（メモリ削減）の要請から、関数を使った乱数生成法が利用される。

【０００４】例えば、関数Ｆが初期値$R_{(0)}$より順番に乱数列$R_{(1)}$、$R_{(2)}$、$R_{(3)}$、…を生成する。個々に、乱数列の（）内の添字は、乱数列Ｒの順番を示すもので、$R_{(i+1)}=F(R_{(i)})$（但し、ｉ≧０、整数）なる関係があるとする。初期値が決まると全ての乱数列が決まるので、理想的な乱数列とは区別し、乱数列$R_{(0)}$、$R_{(1)}$、$R_{(2)}$、$R_{(3)}$、…を疑似乱数列と呼び、Ｆは疑似乱数関数と呼ぶ。

【０００５】上記の乱数生成法における課題は、｜Ｘ｜がＸを取りうる全ての値の個数とすると、$R_{(i+1)}=F(R_{(i)})$で定義される疑似乱数列の周期が上限の｜Ｒ｜にいかに近いかということと、本来の乱数生成の要請

2

である、値の分布が一様にばらつくかどうかということである。

【０００６】図４は、従来の疑似乱数生成装置のブロック図である。同図に示す疑似乱数生成装置１は、レジスタ２及び乱数関数回路３より構成される。レジスタ２は、値Ｒが設定され、外部から起動信号４が入力される毎に、乱数生成回路３から出力される値Ｆによりレジスタ２の蓄積値Ｒを更新し、レジスタ２は、その値Ｆ（Ｒ）を保持する。ここで、レジスタ２の値Ｒの初期設定をしなくてもよいが、多くの場合、電源投入時に値Ｒを蓄積するレジスタ２または、ＲＡＭの物理的な特性により特定値に偏る。また、常に起動信号４が発生する状態にし、値Ｒの更新回数を増大させる方法もある。

【０００７】図５は、従来の疑似乱数生成装置の動作を示すフローチャートである。疑似乱数生成装置１は、外部から起動信号４が入力されるまで、待機し、起動信号４が入力されると（ステップ１）、レジスタの疑似乱数ＲがＦ（Ｒ）で更新される（ステップ２）。

【０００８】また、鍵配送で代表的なＤＨ法（池野、小山著：『現代暗号理論』、電子情報通信学会間、ｐｐ．１７５－１７７）をＡとＢの２者間で行う場合、Ａは、R_A、Ｂは、R_Bなる乱数を生成し、Ａから$\alpha \wedge R_A \bmod P$、Ｂから$\alpha \wedge R_B \bmod P$（なお、Ｘ∧Ｙは、ＸをＹ乗することを表す。Ｘmod Ｙは、ＸをＹで除した余り）を相手に送信する。この結果、両者で共通鍵$K=\alpha \wedge (R_A R_B) \bmod P$を共有する。このとき、悪意の第３者が、$\alpha \wedge R_A \bmod P$、$\alpha \wedge R_B \bmod P$なる通信データを入手し、システムパラメータのα、Ｐを知っても、共有鍵Ｋを生成することはできない。この方法は、Ａまたは、Ｂにおいて、システムに内蔵される疑似乱数装置を用いる。

【０００９】

【発明が解決しようとする課題】しかしながら、図４に示す従来の疑似乱数生成装置は、レジスタに蓄積される値Ｒの初期設定を行わないと、電源投入時にＲを蓄積するレジスタまたは、ＲＡＭの物理的な特性により、特定の値に偏るという問題がある。また、常に、起動信号が入力される状態にし、レジスタの値Ｒの更新回数を増大させる方法は、消費電力削減の点からは好ましくない。

【００１０】さらに、ＤＨ法は、第３者が乱数R_Aを予測できた場合には、Ａと同様に、$\alpha \wedge R_B \bmod P$から共有鍵Ｋを生成できるので、安全な鍵配送が行うことができない。従って、乱数が外部から推測できないことが要請される。

【００１１】一方、一般にシステム中に内蔵される疑似乱数生成装置は、生産上の理由から以下の事象が起きやすい。

（１）大量生産における生産・検査工程の簡単化のため、同じ構造の装置を生産する。

（２）装置の電源を切ると、物理的特性から決まる特定

の値に初期化される。

（３）複数業者へ装置使用の技術開示をすることがあり、構造の秘匿性は確保できない。

【００１２】この結果、例え、疑似乱数列$R_{(0)}$、$R_{(1)}$、$R_{(2)}$、$R_{(3)}$、…が長い周期をもつように疑似乱数関数Ｆが設計されていたとしても、悪意の第３者が装置の電源を切る、または、装置の動作回数を観測することにより、予測する乱数の探索空間を狭めることができ、従来の方法のままでは十分な対策とはなり得ないという問題がある。

【００１３】また、悪意の第３者が正規の通信により、Ａのある時点における乱数Ｒを知り、その後のＡによる乱数の探索空間を狭めることが可能である。例えば、ＲＳＡ暗号により、ＡがＢの正当性を確かめる場合を考える。つまり、Ａが乱数ＲをＢに送り、Ｂは、Ｂの秘密鍵（ｄ，Ｎ）で、

Ｃ←Ｒ∧ｄ　modＮ

を実行し、ＣをＡに送信し、Ｂの公開鍵（ｅ，Ｎ）を用いて、ＡがＣ∧ｅ　modＮを実行し、結果が乱数Ｒに一致するかを確かめる手順を考える。この手順が安全に目的を果たせたとしても、直前のＲの値から続く上記のＤＨ法における乱数が予測できる。

【００１４】これに対する有効な手段は、乱数関数Ｆが乱数Ｒ以外の第２パラメータＫによって変化する関数とし、Ｒ←Ｆ（Ｒ，Ｋ）で疑似乱数列を生成することである。多くの場合、乱数関数Ｆは、暗号関数または、暗号関数を複数組み合わせて構成され、Ｋは、暗号関数の暗号鍵となることが多い。しかしながら、上記のように、乱数の一時の値が外部に既知となると、前後の乱数$R_{(i)}$，$R_{(i+1)}$を観測し、$R_{(i+1)}$＝Ｆ（$R_{(i)}$，Ｋ）となる関数Ｆの入出力から、暗号関数Ｆの既知平文攻撃を構成でき、採用される暗号関数の安全性に全体の安全性が左右され、完全な解決策を与えるに至らない。

【００１５】本発明は、上記の点に鑑みなされたもので、上記従来の問題点を解決し、装置が全く同じ構造、初期化され同じ状態になる、装置使用の技術開示がなされているような条件下でも乱数の秘匿性を確保でき、鍵配送や、相手認証等が安全に実行できる乱数を生成する疑似乱数生成装置を提供することを目的とする。

【００１６】

【課題を解決するための手段】本発明の疑似乱数生成装置は、値Ｃをカウントするカウンタと、値Ｒを蓄積するレジスタと、カウンタの値Ｃ及びレジスタの値Ｒが入力され、乱数関数Ｆ（Ｒ，Ｃ）を出力する乱数生成回路とを具備し、起動信号を契機として乱数生成回路から出力される乱数関数Ｆ（Ｒ，Ｃ）によりレジスタの値Ｒを更新する。

【００１７】また、本発明の上記のカウンタは、内部クロックが起動信号と独立に与えられ、内部クロックに基づいて逐次的にカウンタの値Ｃを更新する。

【００１８】また、本発明の上記の内部クロックは、外部からの観測不能とし、カウンタは、内部クロックに基づいて逐次的にカウンタの値Ｃを更新することにより、外部から与えられる起動信号がカウンタの値Ｃを更新する周期と無関係に与えられる。

【００１９】即ち、本発明の疑似乱数生成装置は、内部クロックに基づいて繰り返し動作するカウンタを自走させ、クロックとは非同期な起動信号または、コマンドによる起動信号を契機に、カウンタ値Ｃを特定して、乱数関数回路から出力される乱数関数Ｆにより、レジスタに蓄積される乱数ＲをＲ←Ｆ（Ｒ，Ｃ）の手続により更新する。

【００２０】

【作用】本発明は、カウンタを起動する内部クロックとは非同期なタイミングで入力される起動信号を利用することにより、外部から観測できないカウンタの値Ｃを用いて、次の乱数Ｒを生成するため、前の乱数の値Ｒに加え、カウンタの値を特定しない限り、悪意の第３者は、その後の乱数は予測することができない。

【００２１】従って、装置使用、初期値等の内部情報が公開し、外部から乱数更新回数を観測しても、正確にカウンタの動きを外部から予測できない。カウンタの値を特定するには、装置内部を観測するまでの工作が必要であり、安全である。

【００２２】

【実施例】以下、図面と共に本発明の実施例を詳細に説明する。

【００２３】図１は、本発明の一実施例の疑似乱数生成装置の構成を示す。同図において、図４と同一構成部分には、同一符号を付与する。疑似乱数生成装置１は、乱数Ｒを蓄積するレジスタ２、乱数関数回路３、起動信号４に加え、内部クロック６に同期して動くカウンタ５が具備される。

【００２４】［第１の実施例］上記の構成により第１の実施例を説明する。

【００２５】第１の実施例は、カウンタ５を内部クロック６に基づいて繰り返し動作させ、内部クロック６とは非同期な外部信号を起動信号４として、カウンタ５の値を特定して乱数関数Ｆによりレジスタ２の値Ｒを更新するものである。

【００２６】図２は、本発明の第１の実施例の疑似乱数生成装置の動作を示すフローチャートである。

【００２７】装置の動作が開始されると、カウンタ５と乱数関数回路３の動作は、同時並行的に行われる。つまり、カウンタ５は、内部クロック６に同期してカウントアップしてＣ←Ｇ（Ｃ）を繰り返す。ここで、関数Ｇは、Ｃ←Ｃ＋１mod Ｔ（Ｔはカウンタの周期）でもよいし、カウンタ５の値Ｃを２進数で一様ランダムな値をとる非線形フィードバックレジスタ構成でもよく、取り得る数値の変動幅（または、２進数表現時のハミング距

離）がランダムに変動してもよい（ステップ１０１）。

【００２８】外部からの起動信号４が入力されると（ステップ１０２）、乱数生成回路３は、レジスタ２の値Ｒとその時点のカウンタ５の値Ｃの値から乱数関数Ｆ（Ｒ，Ｃ）を生成し、この乱数関数でレジスタ２の値Ｒを更新する。

【００２９】起動信号４が内部クロック６と独立に発生することが重要であり、カウンタ５の値Ｃが取り得る値の個数をＴとした場合、予め起動信号４をＬ回起動しておくと、Ｔ∧Ｌ通りの探索空間に広げることができる。

【００３０】従って、初期状態を類推できても、実際に使う疑似乱数の前に予め起動信号をＬ回起動しておくと、Ｔ∧Ｌ通りの探索空間に広げることができる。

【００３１】また、上記の相手確認の場合のように、疑似乱数が直接外部に漏れることがあっても起動信号４をＬ回起動してから疑似乱数を使用することにより、Ｔ∧Ｌ通りの探索空間に広げることができる。

【００３２】［第２の実施例］次に、図１の構成に基づいて、第２の実施例を説明する。

【００３３】第２の実施例は、装置動作がマイクロプロセッサ等によるプログラムによる逐次処理による場合には、カウンタ５と乱数生成回路３の動作は同時並行に行うことができない。このため、カウンタ５の値を逐次的に更新するものである。マイクロプロセッサを用いる場合には、起動信号４としては、コマンドにより契機信号が入力されるものとする。

【００３４】図３は、本発明の第２の実施例の疑似乱数生成装置の動作を示すフローチャートである。

【００３５】カウンタ５は、外部からの起動信号４が入力されない限り、内部クロック６に同期してカウントアップＣ←Ｇ（Ｃ）を繰り返す（ステップ２０１）。外部からの起動信号４が入力された場合に限り（ステップ２０２）、乱数関数回路３は、レジスタ２の値Ｒとその時点のカウンタ５の値Ｃから乱数関数Ｆ（Ｒ，Ｃ）を生成し、この乱数関数によりレジスタ２の値Ｒを更新する（Ｒ←Ｆ（Ｒ，Ｃ））。

【００３６】本実施例では、起動信号４が内部クロック６と独立に発生することが重要であり、前述の第１の実施例と同じ探索空間に広げる効果がある。

【００３７】なお、従来のＲＳＡ暗号により相手認証を行う場合の有効な手段として説明した場合と同様に、疑似乱数関数Ｆは、第２パラメータＣの他に第３パラメータＫを入力して導入し、Ｒ←Ｆ（Ｒ，Ｃ，Ｋ）とすることもできる。

【００３８】上記のように、本実施例によれば、内部クロック６に基づいて繰り返し動作するカウンタ５と、クロックとは非同期な外部からの起動信号による手段により仮に以下の条件が与えられても、

（１）装置が全く同じ構造：

（２）初期化され、同じ状態になる：

（３）装置使用の技術開示：

カウンタ５の取り得る場合の数Ｔと使用前の乱数更新回数Ｌにより探索空欄をＴ∧Ｌ倍に広げることができ、十分な対策となる。

【００３９】また、従来は、ある時点における乱数Ｒを知ることにより、その後の乱数の探索空間を狭めることが可能であったが、上記に実施例によれば、レジスタ２の乱数の更新を適当に行うことで、探索空間をＴ∧Ｌ倍に広げることができる。

【００４０】

【発明の効果】上述のように本発明によれば、装置が全く同じ構造、初期化され同じ状態になる、装置使用の技術開示がなされているような条件下でも、探索空間を広げることにより、乱数の秘匿性を確保でき、鍵配送や、相手認証等が安全に実行できる。

【図面の簡単な説明】

【図１】本発明の一実施例の疑似乱数生成装置の構成図である。

【図２】本発明の第１の実施例の疑似乱数生成装置の動作を占めるフローチャートである。

【図３】本発明の第２の実施例の疑似乱数生成装置の動作を示すフローチャートである。

【図４】従来の疑似乱数生成装置のブロック図である。

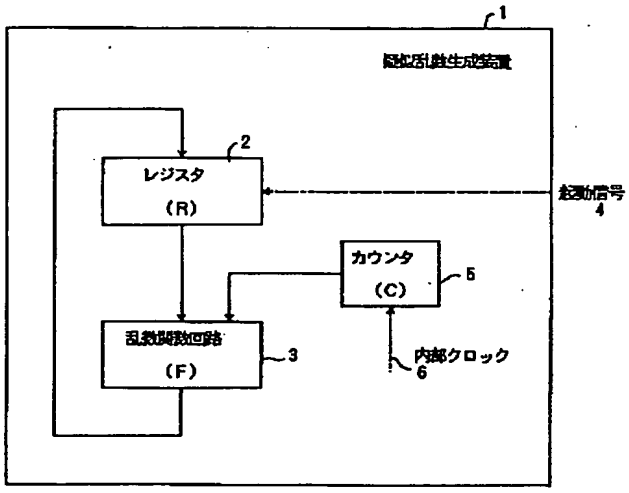
【図５】従来の疑似乱数生成装置の動作を示すフローチャートである。

【符号の説明】

１　疑似乱数生成装置
２　レジスタ
３　乱数関数回路
４　起動信号
５　カウンタ
６　内部クロック

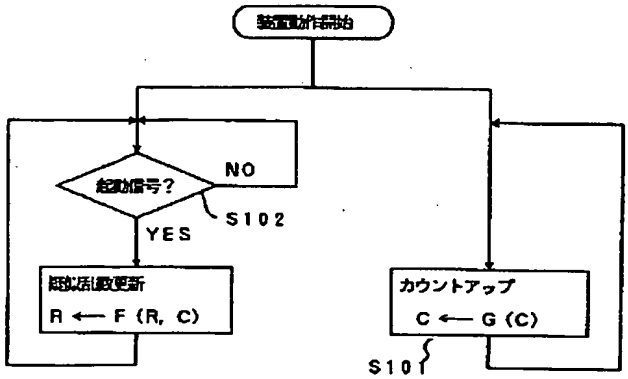
【図１】

本発明の一実施例の疑似乱数生成装置の構成図



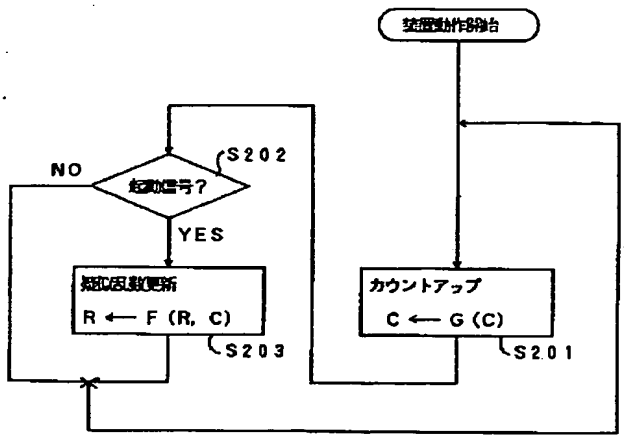
【図２】

本発明の第１の実施例の疑似乱数生成装置の動作を示すフローチャート



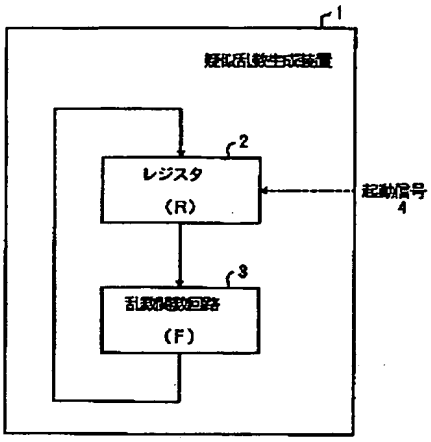
【図３】

本発明の第２の実施例の疑似乱数生成装置の動作を示すフローチャート



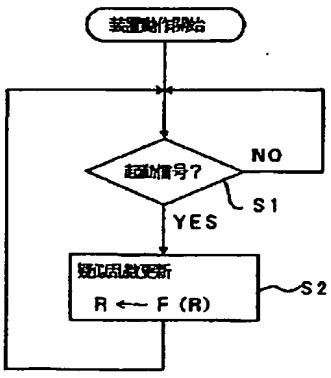
【図４】

従来の疑似乱数生成装置のブロック図



【図５】

従来の疑似乱数生成装置の動作を示すフローチャート



フロントページの続き

(51) Int. Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｌ	9/10				
	9/12				